424 Rec'd PCT/PTO 26 MAY 2000

FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NO. PHD 99-097
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	U.S. Application No. (if known, see 37 CFR 1.5) 09/555301

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/07026	SEPTEMBER 21, 1999	SEPTEMBER 30, 1998 and August 5, 1999

TITLE OF INVENTION
DATA PROCESSING DEVICE AND METHOD FOR OPERATING SAME WHICH PREVENTS A DIFFERENTIAL CURRENT CONSUMPTION ANALYSIS

APPLICANT(S) FOR DO/EO/US
MARKUS FEUSER

Applicant(s) herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.

2. [ ] This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.

3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).

4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] A copy of the International Application as filed (35 U.S.C. 371 (c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).

6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2))

7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.

8. [ ] A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).

9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. Below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.

12. [X] An assignment document for recording. A separate cover sheet is compliance with 37 C.F.R. 3.28 and 3.31 is included.

13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND OR SUBSEQUENT preliminary amendment.

14. [ ] A substitute specification.

15. [ ] A change of power of attorney and/or address letter.

16. [X] Other items or information:
    Charge Authorization

EL297131917US

MAY 26, 2000

Josephine Cangelosi

S:\pw\mu25pwt0.cn0

Josephine Cangelosi

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/555301	PCT /EP99/07026	PHD 99-097

17 [x] The following fees are submitted:		CALCULATIONS (PTO USE ONLY)
BASIC NATIONAL FEE (37 C.F.R. 1.492(A)(1)-(5)):		
Search Report has been prepared by the EPO or JPO	$940.00	
International preliminary-examination fee paid to USPTO (37 C.F.R. 1.482)	$720.00	
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)	$760.00	
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO	$970.00	
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	$ 96.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$970.00

Surcharge of $130.00 for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	4 - 20 =		X $ 18.00	$	
Independent claims	2 - 3 =		X $ 78.00	$	
MULTIPLE DEPENDENT CLAIMS (if applicable)			+ $260.00	$	
TOTAL OF ABOVE CALCULATIONS =				$970.00	
Reductions by 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 C.F.R. 1.9, 1.27, 1.28)				$	
SUBTOTAL =				$970.00	
Processing fee of $130.00 for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28,3.31). $40.00 per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$1,010.00	
				Amount to be Refunded	$
				Charged	$

a. [ ] A check in the amount $_____ to cover the above fees is enclosed.

b. [X] Please charge my Deposit Account No. 14-1270 in the amount of $ 1,010.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fee, with the exception of the Base Issue Fee, which may be required, or credit any overpayment to Deposit Account No. 14-1270. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.496 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Corporate Patent Counsel
Philips Electronics North America Corporation
580 White Plains Road
Tarrytown, NY 10591

(SIGNATURE)

Daniel J. Piotrowski
(NAME)

42,079
(REGISTRATION NUMBER)

DATE OF MAILING:

5/26/00

S:\pw\mu25pwt0.cn0

Data processing device and method for operating same which prevents a differential current consumption analysis

Technical field

The invention relates to a method of operating a data processing device, notably a chip card, which includes an integrated circuit which carries out, in dependence on a clock signal, arithmetic operations, notably cryptographic operations, data input and data output as well as data transfer between registers of the integrated circuit as disclosed in the introductory part of Claim 1. The invention also relates to a data processing device, notably a chip card, which is specifically intended to carry out the method and includes an integrated circuit which executes arithmetic operations, notably cryptographic operations, in dependence on a clock signal, the integrated circuit including a processor with an associated first register and data inputs and outputs as disclosed in the introductory part of Claim 3.

State of the art

In many data processing apparatus provided with an integrated circuit, for example, cryptographic operations are carried out so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or IC card. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

Arithmetic operations performed by the integrated circuit, for example in order to calculate cryptographic algorithms, involve the formation of logic combinations of operands or intermediate results. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the

Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus. "Differential Power Analysis" thus enables the extraction of additional internal information of an integrated circuit beyond pure functionality.

From US 5 297 201 it is known to combine a high frequency radiating computer with a device which also radiates high frequency similar to that of the computer. Thus, an unauthorized third party can no longer decode the high-frequency radiation of the computer. Crypto analysis by a third party having direct access to the computer, however, cannot be prevented by this system.

WO 90/15489 describes a protected communication system in which dummy traffic or dummy transfers are produced so as to impede cryptographic analysis. Crypto analysis by a third party having direct access to the computer, however, cannot be prevented either by this system.

Implementation of the invention, object, solution, advantages

It is an object of the present invention to provide an improved method and an improved data processing device of the kind set forth which eliminate the described drawbacks and offer effective protection against "Differential Power Analysis".

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1, and by means of a data processing device of the kind set forth which is characterized as disclosed in Claim 3.

To this end, in conformity with the method of the kind set forth according to the invention the integrated circuit is controlled in such a manner that the execution of arithmetic operations on the one hand and the data input/output as well as the data transfer from one register to another or between registers on the other hand is executed in parallel in time.

This offers the advantage that the differential power analysis does not have any clue as to when an arithmetic operation ends or when reading out/writing of registers takes place or when data input/output takes place, because periods of time of the actual calculations as well as the data input and data output are disguised. Differential power analysis is thus significantly obstructed, because it is no longer possible to determine from the outside whether a real calculation takes place or an input/output operation.

In order to disguise the arithmetic operations as well as data inputs/outputs even further, in a further version of the method dummy calculations are performed by a processor of the integrated circuit directly before, during and/or directly after the data transfer between the registers of the integrated circuit, which dummy calculations act on random or predetermined data, and no data are written into registers of the integrated circuit.

A data processing device of the kind set forth according to the invention is provided with a second register which is connected to the first register and includes the data inputs and outputs, and a control unit is connected to the integrated circuit, the control unit being constructed in such a manner that it controls parallel operation in time of the registers for data input/output and data transfer between the registers on the one hand and arithmetic operations of the processor on the other hand.

This offers the advantage that the differential power analysis does not have any clue as to when an arithmetic operation ends or when reading-out/writing of registers takes place or when data input/output takes place, because periods of time of the actual calculations as well as the data input and data output are disguised. The second register enables input/output of data while the processor is active and possibly writes data into the first register or reads out data from the first register. Differential power analysis is thus significantly obstructed because, when the second register is suitably controlled, it is no longer possible to determine from the outside whether a real calculation takes place or an input/output operation.

The first register in an advantageous further embodiment of the data processing device is an operand register of the processor and/or the second register is an operand register for the data input/output.

Preferred description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein:

Fig. 1 shows a block diagram of a preferred embodiment of a data processing device according to the invention,

Fig. 2 shows a block diagram of an integrated circuit of the data processing device of Fig. 1,

Fig. 3 graphically illustrates the activity of the data processing device according to the invention as a function of time according to the present state of the art, and

Fig. 4 graphically illustrates the activity of the data processing device according to the invention as a function of time in accordance with the invention.

Preferred implementation of the invention

Fig. 1 shows a preferred embodiment of a data processing device 100 according to the invention which includes an integrated circuit 10, a register 12 with program access 14 and a control unit 16. Via the lead 18, the control unit 16 and the integrated circuit receive a clock signal 20 as shown in the Figs. 3 and 4. Via control leads 22, the control unit 16 controls the integrated circuit 10 which includes data inputs 24 and data outputs 26.

As is shown in Fig. 2, the integrated circuit 10 includes a processor 28, a first operand register 30 which is associated with the processor 28 and a second operand register 32 which is connected to the first operand register 30. The second operand register 32 isprovided with the data inputs 24 and the data outputs 26. The clock signal 20 (Figs. 3 and 4) is applied, via the lead 18, to the processor 28 as well as to the two operand registers 30 and 32. During the execution of calculations or operations by the processor 28, it reads out data from the first register 30 or writes a result of a calculation into the first register 30. A data exchange or a mutual transfer of data, referred to hereinafter as R2-1, takes place between the registers 30 and 32 when data is transferred from the second register 32 to the first register 30 or, referred to as R1-2, when data is transferred from the first register 30 to the second register 32. A control lead 22, originating from the control unit 16, is connected to the second register 32 for the purpose of control whereas a further control lead 22 is connected to the first register 30 for the purpose of control.

According to an article "Differential Power Analysis" published by Paul Kocher on the Internet under http://www.cryptography.com/dpa: not only the input/output signals are analyzed but also a current consumption I_a or voltage drops ΔU_a of a supply voltage U_a of the integrated circuit. The success of this method of analysis is dependent on whether a number N_A of analog ($I_a(t)$ or $\Delta U_a(t)$) signal variations S(k,t) in time can be measured with

$k = \{1,...,N_A\}$ different operands in such a manner that it is possible to form a sum of the form:

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k).S(k,t)$$

with the coefficients p(i,k), where $i = \{0,1, 2,...\}$. When different signal variations $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$ ... are observed at the same instant $t = t_1$, differential power analysis can be succesful only if the integrated circuit executes the same arithmetic operation with different operands $k = \{1,...,N_A\}$ at that instant, i.e. it must be possible to make the signal variations S(k,t) register exactly. This holds not only for the calculation itself, but also for the input and output of data.

The invention disguises the periods of time of the actual calculation as well as the periods of time of the data input or data output. When the second register 32 is suitably controlled, it can no longer be detected from the outside when an actual calculation or an input/output takes place. Differential power analysis is thus significantly obstructed. The integrated circuit 10 according to the invention is provided with the two operand registers 30 and 32. This enables input and output of data via the second operand register 32, having the data inputs 24 and data outputs 26, also while the processor 28 is active in executing calculations or operations while using the first operand register 30.

Fig. 4 illustrates a mode of operation of the data processing device 100 and shows the clock signal 20 and a mode of operation of the processor and the operand registers on a time base 34. The reference numeral 36 denotes a mode of operation in which the processor executes a calculation. The reference numeral 38 denotes a mode of operation in which a data input or data output takes place; the reference numeral 40 denotes a mode of operation in which a data transfer R1-2 takes place while the reference numeral 42 denotes a mode of operation in which a data transfer R2-1 takes place.

Fig. 3 shows, in the same way as Fig. 4, a mode of operation of a conventional data processing device. Therein, the input and output phases 38 precede and succeed, respectively, the actual calculation 36 in time. The phases with the calculations 36 and the input/output 38 can be readily identified by means of differential power analysis; it can notably be detected which inputs 38 takes place during a calculation 40 and what outputs 38 result.

In the mode of operation according to the invention as shown in Fig. 4, the control unit 16 disguises the calculations 36 as well as the data inputs/outputs 38, 40, 42 by

controlling the data flow of the two operand registers 30, 32 so as to be parallel in time with the calculations 36. Calculations 36 always take place. However, the copying actions R1-2 40 and R2-1 42 now determine whether a calculation 40 is dependent on the input 38 or produces an output 38. The calculations before R2-1 42 and after R1-2 40 are, for example, dummy calculations. Dummy arithmetic operations are calculation operations which act on predetermined input data or random input data, the result being rejected and not taken up in the results or input data for the actual arithmetic operations. Additional dummy inputs/outputs can be optionally provided. The dummy calculations as well as the dummy inputs/dummy outputs produce current or voltage variations which are very similar to those of the actual calculations and inputs/outputs.

The control unit 16, provided according to the invention for the protection of the integrated circuit 10 against differential power analysis, is aimed specifically at the input/output phases 38, 40, 42 of calculations 36 to be performed in the circuit elements 10 by way of digital, electronic signal processing, because inputs/outputs could also be analyzed by differential power analysis of the current consumption. Thus, for differential power analysis it is of interest to know when a calculation 36 starts or ends. It is exactly this information in the current consumption signal that is suppressed in the method and the device according to the invention.

CLAIMS:

1. A method of operating a data processing device (100), notably a chip card, which includes an integrated circuit (10) which carries out, in dependence on a clock signal, arithmetic operations, notably cryptographic operations, data input and data output (38) as well as data transfer (40) from and to registers of the integrated circuit (10),
characterized in that
the integrated circuit (10) is controlled in such a manner that the execution of arithmetic operations on the one hand and the data input/output (38) as well as the data transfer (40) from one register to another or between registers (30, 32) on the other hand is executed in parallel in time.

2. A method as claimed in Claim 1,
characterized in that
directly before, during and/or directly after the data transfer from one register to another or between the registers (30, 32) of the integrated circuit, a processor (28) of the integrated circuit (10) executes dummy calculations which act on random or predetermined data, no data being written into registers (30, 32) of the integrated circuit.

3. A data processing device (100), notably a chip card, which is specifically intended to carry out a method as claimed in at least one of the preceding Claims, and includes an integrated circuit (10) which executes arithmetic operations, notably cryptographic operations, in dependence on a clock signal (20), the integrated circuit (10) including a processor (28) with an associated first register (30) and data inputs and outputs (24, 26),
characterized in that
a second register (32) is connected to the first register (30) and is provided with the data inputs and outputs (24, 26), a control unit (16) being connected to the integrated circuit (10) and being constructed in such a manner that it controls parallel operation in time of the registers (30, 32) for data input/output (38) and data transfer (40) from register to register or

between the registers (30, 32) on the one hand and arithmetic operations (40) of the processor (28) on the other hand.

4. A data processing device (100) as claimed in Claim 3,

characterized in that

the first register (30) is an operand register of the processor (28) and/or the second register (32) is an operand register for the data input/output (38).

LIST OF REFERENCES

100	data processing device
10	integrated circuit
12	register
14	program access
16	control unit
18	lead
20	clock signal
22	control leads
24	data inputs
26	data outputs
28	processor
30	first operand register R1
32	second operand register R2
34	time base
36	calculation
38	data input and data output
40	data transfer R1-2
42	data transfer R2-1

ABSTRACT:

The present invention relates to a data processing device (100) as well as to a method of operating a data processing device, notably a chip card, which includes an integrated circuit which executes, in dependence on a clock signal, arithmetic operations, notably cryptographic operations, data inputs and data outputs as well as data transfer from and to registers of the integrated circuit. The integrated circuit (10) is controlled in such a manner that the execution of arithmetic operations on the one hand and the data input/output as well as the data transfer from register to register or between registers on the other hand are carried out in parallel in time.

(Fig. 1)

Fig.1

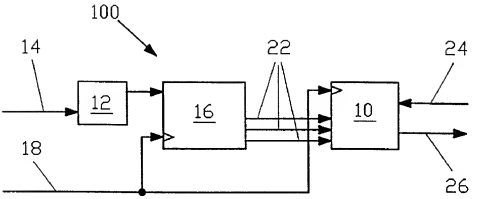


Fig.2

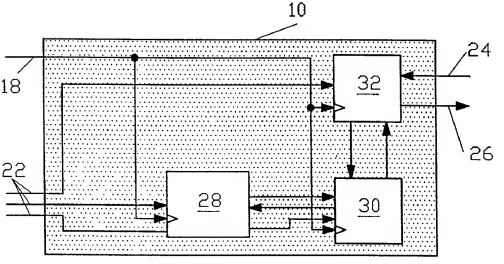


Fig.3

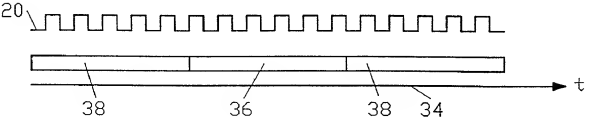
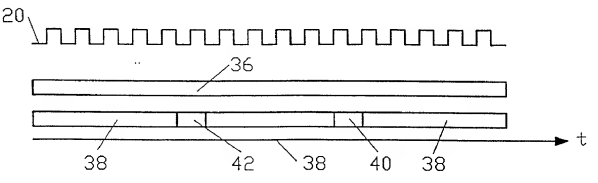


Fig.4



COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
(includes Reference to PCT International Applications)

ATTORNEY'S DOCKET NUMBER
PHD 99.097 US

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which aa patent is sought on the invention entitled: "Data processing device and method for operating same which prevents a differential current consumption analysis"

the specification of which (check only one item below):

☐ is attached hereto.

☐ was filed as United States application

Serial No

on

and was amended

on

☒ was filed as PCT international application

Number PCT/EP99/07026

on 21 September 1999 (21.09.99)

and was amended under PCT Article 19

on (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 USC 119
Germany	**19844992.5**	**30 September 1998**	**YES**
Germany	**19936939.9**	**5 August 1999**	**YES**

09/555301
526 Rec'd PCT/PTO 26 MAY 2000

Combined Declaration For Patent Application and Power of Attorney (Continued)
(includes Reference to PCT International Applications)

Attorneys Docket Number
PHD 99.097 US

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) abnd/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

Algy Tamoshunas Reg. No. 27,677
Jack E. Haken, Reg. No. 26,902

Direct Telephone Calls to:
(name and telephone number)
(914)332-0222

201	FULL NAME OF INVENTOR	FAMILY NAME **FEUSER**	FIRST GIVEN NAME **Markus**	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY **Buchholz**	STATE OR FOREIGN COUNTRY **Germany** DEX	COUNTRY OF CITIZENSHIP **Germany**
	POST OFFICE ADDRESS	POST OFFICE ADDRESS **Hamburger Str. 4c**	CITY **21244 Buchholz**	STATE & ZIP CODE/COUNTRY **Germany**
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
203	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
204	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
205	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
206	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 if Title 18 of the United states Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Markus Feuser		
DATE April 20, 2000	DATE	DATE
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
DATE	DATE	DATE